BIOMETRIC IDENTIFICATION SYSTEMS: FEATURE LEVEL CLUSTERING OF LARGE BIOMETRIC DATA AND DWT BASED HASH CODED EAR BIOMETRIC SYSTEM

Thesis submitted in partial fulfillment of the requirements for the award of the degree.

of

Bachelor of Technology (Computer Science and Engg.)

By:

V.BHAWANI RADHIKA

10506022

Department of Computer Science and Engineering
National Institute of Technology
(DEEMED UNIVERSITY)
ROURKELA

National Institute of Technology Rourkela
Rourkela-769008

CERTIFICATE

This is to certify that the work in this Thesis Report entitled "BIOMETRIC IDENTIFICATION SYSTEMS: FEATURE LEVEL CLUSTERING OF LARGE BIOMETRIC DATA AND DWT BASED HASH CODED EAR BIOMETRIC SYSTEM"" by V.BHAWANI RADHIKA in partial fulfillment of the requirements for the degree of ***Bachelor of Technology*** in Computer Science during session 2005-2009 in the Department of Computer Science and Engineering, National Institute of Technology Rourkela, and is an authentic work under my supervision and guidance.

To the best of my knowledge, the matter embodied in the thesis has not been submitted to any other University/Institute for the award of any Degree or Diploma

Place:Rourkela
Date:May 11, 2009

Dr. B. Majhi
Professor and Head
Dept of Computer Science and Engg
National Institute of Technology
Rourkela-769008

ACKNOWLEDGEMENTS

No thesis is created entirely by an individual, many people have helped to create this thesis and each of their contribution has been valuable. I express my sincere gratitude to my thesis supervisor, *Prof. B.Majhi Prof and Head Dept of Computer Science and Engineering,* for his kind and able guidance for the completion of the thesis work. His consistent support and intellectual guidance made me energize and innovate new ideas.

Last, but not least I would like to thank all professors and lecturers, and members of the department of Computer Science, Engineering, National. Institute of Technology, Rourkela for their generous help in various ways for the completion of this thesis.

(V.BHAWANI RADHIKA)

B.TECH

COMPUTER SCIENCE & ENGG

2005-2009

CONTENTS

LIST OF FIGURES

.

ABSTRACT

Biometrics is the science of measuring physical properties of living beings. It is the automated recognition of individuals based on their behavioral and biological characteristics. Biometric features are information extracted from biometric samples which can be used for comparison with a biometric reference. The aim of the extraction of biometric features from a biometric sample is to remove any superfluous information which does not contribute to biometric recognition. This enables a fast comparison, an improved biometric performance, and may have privacy advantages. In an automated biometric system, the identity of an individual is established by measuring an individual's suitable behavioral and biological characteristics in a recognition inquiry and comparing these data with the biometric reference data which had been stored during a learning procedure. To be able to recognize a person by their biometric characteristics and the derived biometric features, first a learning phase must take place. The procedure is called enrolment and comprehends the creation of an enrolment data record of the biometric data subject (the person to be enrolled) and to store it in a biometric enrolment database. The enrolment data record comprises one or multiple biometric references and arbitrary non-biometric data such as a name or a personnel number. For the purpose of recognition, the biometric data subject (the person to be recognized) presents his or her biometric characteristic to the biometric capture device which generates a recognition biometric sample from it. From the recognition biometric sample the biometric feature extraction creates biometric features which are compared with one or multiple biometric templates from the biometric enrolment database. Due to the statistical nature of biometric samples there is generally no exact match possible. For that reason, the decision process will only assign the biometric data subject to a biometric template and confirm recognition if the comparison score exceeds an adjustable threshold.
In the development of biometric identification systems, physical and behavioral characteristics for recognition are required-which dispose of biometric features which are as unique as possible, i.e., which do not reappear at any other person, which occur in as many people as possible, whose biometric features don't change over time, which are measurable with simple technical instruments, which are easy and comfortable to measure.

Conventional Biometric Modalities include Fingerprint Finger lines, pore structure Signature (dynamic) Writing with pressure and speed differentials Facial geometry Distance of specific facial features (eyes, nose, mouth) Iris pattern Retina Eye background (pattern of the vein structure) Hand geometry Measurement of fingers and palm Finger geometry Finger measurement Vein structure of hand Vein structure of the back or palm of the hand or a finger Ear form Dimensions of the visible ear Voice Tone or timbre DNA code as the carrier of human hereditary Odor Chemical composition of the one's odor Keyboard strokes Rhythm of keyboard strokes (PC or other keyboard)

Here we propose a new identification strategy for signature databases and an efficient recognition technique for ear biometrics. This paper proposes an efficient technique for partitioning large biometric database during identification. In this technique feature vector which comprises of global and local descriptors extracted from offline signature are used by fuzzy clustering technique to partition the database. As biometric features posses no natural order of sorting, thus it is difficult to index them alphabetically or numerically. Hence, some supervised criteria is required to partition the search space. At the time of identification the fuzziness criterion is introduced to find the nearest clusters for declaring the identity of query sample. The system is tested using bin-miss rate and performs better in comparison to traditional k-means approach.

Biometric authentication systems are fast replacing conventional identification schemes such as passwords and PIN numbers. This paper introduces a novel matching scheme that uses a image hash scheme. It uses Discrete Wavelet Transformation (DWT) of biometric images and randomized processing strategies for hashing. In this scheme the input image is decomposed into approximation, vertical, horizontal and diagonal coefficients using the discrete wavelet transform. The algorithm converts images into binary strings and is robust against compression, distortion and other transformations. As a case study the system is tested on ear database and is outperforming with an accuracy of 96.37% with considerably low FAR of 0.17%. The performance shows that the system can be deployed for high level security applications.

CHAPTER 1: INTRODUCTION TO BIOMETRIC SYSTEMS

1.1 INTRODUCTION

Biometrics is a general term used alternatively to describe a characteristic or a process. As a characteristic, a biometric is a measurable biological (anatomical and physiological)or behavioral characteristic that can be used for automated recognition. As a process it is an automated method of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

Biometrics commonly implemented or studied includes fingerprint, face, iris, voice, signature, and hand geometry. Many other modalities are in various stages of development and assessment. There is not one biometric modality that is best for all implementations. Many factors must be taken into account when implementing a biometric device including location, security risks, task (identification or verification), expected. Biometrics are typically collected using a device called a sensor. These sensors are used to acquire the data needed for recognition and to convert the data to a digital form. The quality of the sensor used has a significant impact on the recognition results. Example “sensors” could be digital cameras (for face recognition) or a telephone (for voice recognition) [1].

A biometric template is a digital representation of an individual’s distinct characteristics, representing information extracted from a biometric sample. Biometric templates are what are actually compared in a biometric recognition system. Templates can vary between biometric modalities as well as vendors. Not all biometric devices are template based. For example, voice recognition is based on “models.”

Biometrics are being used in many locations to enhance the security and convenience of the society. Example deployments within the United States Government include the FBI’s IAFIS, the US-VISIT program, the Transportation Workers Identification Credentials (TWIC) program, and the Registered Traveler (RT) program. These deployments are intended to strengthen the security and convenience in their respective environments. Many companies are also implementing biometric technologies to secure areas, maintain time records, and enhance user convenience. For example, for many years Disney World has employed biometric devices for season ticket holders to expedite and simplify the process of entering its parks.

- **MOTIVATION**

We propose an efficient technique for partitioning large biometric database during identification. In this technique feature vector which comprises of global and local descriptors extracted from offline signature are used by fuzzy clustering technique to partition the database. As biometric

features posses no natural order of sorting, thus it is difficult to index them alphabetically or numerically. Hence, some supervised criteria is required to partition the search space. At the time of identification the fuzziness criterion is introduced to find the nearest clusters for declaring the identity of query sample. The system is tested using bin-miss rate and performs better in comparison to traditional k-means approach.

Biometric authentication systems are fast replacing conventional identification schemes such as passwords and PIN numbers. We introduce a novel matching scheme that uses a image hash scheme. It uses Discrete Wavelet Transformation (DWT) of biometric images and randomized processing strategies for hashing. In this scheme the input image is decomposed into approximation, vertical, horizontal and diagonal coefficients using the discrete wavelet transform. The algorithm converts images into binary strings and is robust against compression, distortion and other transformations. As a case study the system is tested on ear database.

- **ORGANIZATION OF THE THESIS**

The rest of the thesis is organized as follows. Chapter 1 provides an introduction to biometrics. Chapter 2 overlays an application of fuzzy clustering on signature databases Chapter 3 discusses a hash coded ear biometric system. Chapter 4 provides the experimental results and conclusion.

1.2 BIOMETRICS IDENTIFICATION SYSTEMS

Associating an identity with an individual is called personal identification. The problem of resolving the identity of a person can be categorized into two fundamentally distinct types of problems with different inherent complexities:

- Verification and
- Recognition (more popularly known as identification).

Verification (authentication) refers to the problem of confirming or denying a person's claimed identity (Am I who I claim I am?). Identification (Who am I?) refers to the problem of establishing a subject's identity - either from a set of already known identities (closed identification problem) or otherwise (open identification problem).

Recognition is a generic term, and does not necessarily imply either verification or identification. All biometric systems perform “recognition” to “again know” a person who has been previously enrolled, Verification is a task where the biometric system attempts to confirm an individual’s claimed identity by comparing a submitted sample to one or more previously enrolled templates.

The term *positive personal identification* typically refers (in both verification as well as identification context) to identification of a person with high certainty. Human race has come a long way since its inception in small tribal primitive societies where every person in the community knew every other person. In today's complex, geographically mobile, increasingly electronically inter-connected information society, accurate identification is becoming very important and the problem of identifying a person is becoming ever increasingly difficult. A number of situations require an identification of a person in our society: have I seen this applicant before? Is this person an employee of this company? Is this individual a citizen of this country? Many situations will even warrant identification of a person at the far end of a communication channel.

The general problem of personal identification raises a number of important research issues: what identification technologies are the most effective to achieve accurate and reliable identification of individuals? Some of these problems are well-known open problems in the allied areas (e.g., pattern recognition and computer vision), while the others need a systematic cross-disciplinary effort [1].

1.3 CHARACTERISTICS OF BIOMETRIC SYSTEMS

Any human physiological or behavioral characteristic could be a biometrics provided it has the following desirable properties:

1. *Universality*, which means that every person should have the characteristic,
2. *Uniqueness*, which indicates that no two persons should be the same in terms of the characteristic,
3. *Permanence*, which means that the characteristic should be invariant with time
4. C*ollectability*, which indicates that the characteristic can be measured quantitatively.

In practice, there are some other important requirements :

1. *Performance*, which refers to the achievable identification accuracy, the resource requirements to achieve an acceptable identification accuracy, and the working or environmental factors that affect the identification accuracy,
2. A*cceptability*, which indicates to what extent people are willing to accept the biometric system, and
3. C*ircumvention*, which refers to how easy it is to fool the system by fraudulent techniques[1].

1.4 BIOMETRIC MODALITIES

No single biometrics is expected to effectively satisfy the needs of all identification (authentication) applications. A number of biometrics have been proposed, researched, and evaluated for identification (authentication) applications. Each biometrics has its strengths and limitations; and accordingly, each biometric appeals to a particular application. The distinction between the terms biometrics and biometry is that- biometry encompasses a much broader field involving application of statistics to biology and medicine.

A summary of the existing and burgeoning biometric technologies is described in this section[1].

1.4.1 VOICE

Voice is a characteristic of an individual . However, it is not expected to be sufficiently unique to permit identification of an individual from a large database of identities .A voice signal is shown

in Figure 1.1.A voice signal available for authentication is typically degraded in quality by the microphone, communication channel, and digitizer characteristics. Before extracting features, the amplitude of the input signal may be normalized and decomposed into several band-pass frequency channels. The features extracted from each band may be either time-domain or frequency domain features. One of the most commonly used features is spectral feature - which is a logarithm of the Fourier Transform of the voice signal in each band. The matching strategy may typically employ approaches based on hidden Markov model, vector quantization, or dynamic time warping . Text dependent speaker verification authenticates the identity of a subject based on a fixed predetermined phrase. Text-independent speaker verification is more difficult and verifies a speaker identity independent of the phrase. Language independent speaker verification verifies a speaker identity irrespective of the language of the uttered phrase and is even more challenging.

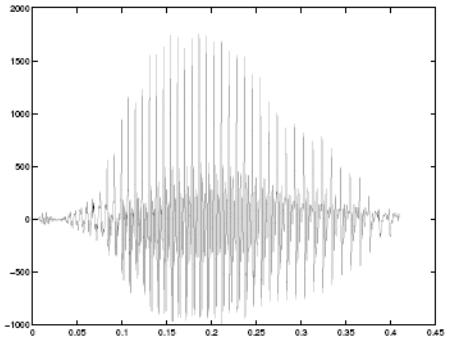


Figure 1.1 Voice signal representing an utterance of the word .X and Y axes represent time and signal amplitude, respectively.

Voice capture is unobtrusive and voice print is an acceptable biometric in almost all societies. Some applications entail authentication of identity over telephone. In such situations, voice may be the only feasible biometric. Voice is a behavioral biometrics and is affected by a person's health (e.g., cold), stress, emotions, etc. To extract features which remain invariant in such cases is very difficult. Besides, some people seem to be extraordinarily skilled in mimicking others. A reproduction of an earlier recorded voice can be used to circumvent a voice authentication system in the remote unattended applications. One of the methods of combating this problem is to prompt the subject (whose identity is to be authenticated) to utter a different phrase each time.

1.4.2 INFRARED FACIAL AND HAND VEIN THERMOGRAMS

The image is obtained by sensing the infrared radiations from the face of a person. The gray level at each pixel is characteristic of the magnitude of the radiation. Human body radiates heat and the pattern of heat radiation is a characteristic of each individual body . An infrared sensor could acquire an image indicating the heat emanating from different parts of the body .These images are called thermograms (Figure 1.2).

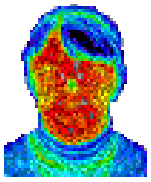


Figure 1.2 Identification based on facial thermograms .

The method of acquisition of the thermal image unobtrusively is akin to the capture of a regular (visible spectrum) photograph of the person. Any part of the body could be used for identification. The absolute values of the heat radiation are dependent upon many extraneous factors and are not completely invariant to the identity of an individual; the raw measurements of heat radiation need to be normalized, e.g., with respect to heat radiating from a landmark feature of the body. The technology could be used for covert identification solutions and could distinguish between identical twins. It is also claimed to provide enabling technology for identifying people under the influence of drugs: the radiation patterns contain signature of each narcotic drug . A thermogram-based system may have to address sensing challenges in uncontrolled environments, where heat emanating surfaces in the vicinity of the body, e.g., room heaters and vehicle exhaust pipes, may drastically affect the image acquisition phase. Infrared facial thermograms seem to be acceptable since their acquisition is a non-contact and non-invasive sensing technique. Identification systems using facial thermograms are commercially available. A related technology using near infrared imaging is used to scan the back of a clenched fist as shown in Figure 1.3 to determine hand vein structure .Infrared sensors are prohibitively expensive which is a factor inhibiting wide spread use of thermograms.

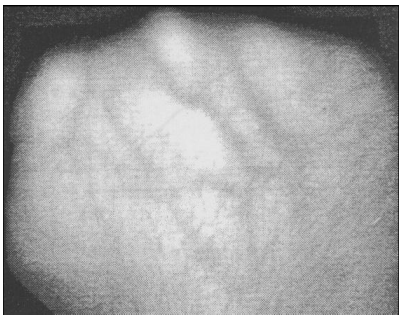


Figure 1.3 Identification based on hand veins .

1.4.3 FINGERPRINTS

Fingerprints are graphical flow-like ridges present on human fingers(Figure 1.4). Their formations depend on the initial conditions of the embryonic development and they are believed to be unique to each person (and each finger). Fingerprints are one of the most mature biometric technologies used in forensic divisions worldwide for criminal investigations and therefore, have a stigma of criminality associated with them. Typically, a fingerprint image is captured in one of two ways:

(i) Scanning an inked impression of a finger or

(ii) Using a live-scan fingerprint scanner .

(a) (b)

Figure 1,4 A fingerprint image could be captured from the inked impression of a finger or directly imaging a finger using frustrated total internal reflection technology. The former is called an inked fingerprint (a) and the latter is called a live-scan fingerprint (b).

Major representations of the finger are based on the entire image, finger ridges, or salient features derived from the ridges (minutiae).

Four basic approaches to identification based on fingerprint are prevalent:

(i) The invariant properties of the gray scale profiles of the fingerprint image or a part thereof;

(ii) Global ridge patterns, also known as fingerprint classes;

(iii) The ridge patterns of the fingerprints;

(iv) Fingerprint minutiae – the features resulting mainly from ridge endings and bifurcations.

1.4.4 FACE

Face is one of the most acceptable biometrics because it is one of the most common method of identification which humans use in their visual interactions(Figure 1.5). In addition, the method of acquiring face images is non-intrusive.

Two primary approaches to the identification based on face recognition are the following:

- Transform approach : The universe of face image domain is represented using a set of orthonormal basis vectors. Currently, the most popular basis vectors are eigenfaces: each eigenface is derived from the covariance analysis of the face image population; two faces are considered to be identical if they are sufficiently “close” in the eigenface feature space. A number of variants of such an approach exist.
- (Attribute-based approach : Facial attributes like nose, eyes, etc. are extracted from the face image and the invariance of geometric properties among the face landmark features is used for recognizing features. Facial disguise is of concern in unattended authentication applications. It is very challenging to develop face recognition techniques which can tolerate the effects of aging, facial expressions, slight variations in the imaging environment and variations in the pose of face with respect to camera (2D and 3D rotations).

Figure 1.5 Identification based on face is one of the most acceptable methods of biometric based identification.

1.4.5 IRIS

Visual texture of the human iris (Figure 1.6) is determined by the chaotic morphogenetic processes during embryonic development and is posited to be unique for each person and each eye . An iris image is typically captured using a non-contact imaging process .The image is obtained using an ordinary CCD camera with a resolution of 512 dpi. Capturing an iris image involves cooperation from the user, both to register the image of iris in the central imaging area and to ensure that the iris is at a predetermined distance from the focal plane of the camera. A position-invariant constant length byte vector feature is derived from an annular part of the iris image based on its texture. The identification error rate using iris technology is believed to be extremely small and the constant length position invariant code permits an extremely fast method of iris recognition.

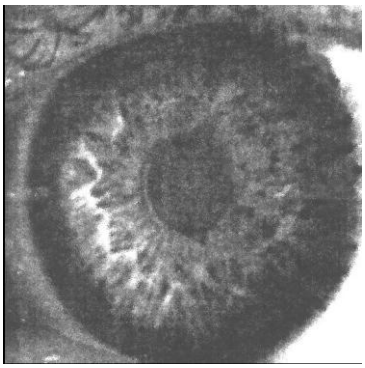


Figure 1.6 Identification Based on Iris.

1.4.6 EAR

It is known that the shape of the ear and the structure of the cartilegenous tissue of the pinna are distinctive (Figure 1.7). The features of an ear are not expected to be unique to each individual. The ear recognition approaches are based on matching vectors of distances of salient points on the pinna from a landmark location on the ear. No commercial systems are available yet and authentication of individual identity based on ear recognition is still a research topic.

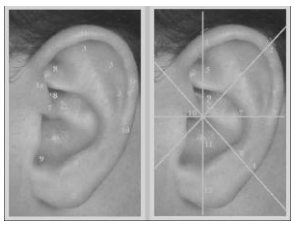


Figure 1.7 An image of an ear and the features used for ear-based identification .

1.4.7 GAIT

Gait is the peculiar way one walks and is a complex spatio-temporal behavioral biometrics. Gait is not supposed to be unique to each individual, but is sufficiently characteristic to allow identity authentication(Figure 1.8). Gait is a behavioral biometric and may not stay invariant especially over a large period of time, due to large fluctuations of body weight, major shift in the body weight (e.g., waddling gait during pregnancy , major injuries involving joints or brain (e.g., cerebellar lesions in Parkinson disease), or due to inebriety (e.g., drunken gait).

Figure 1.8 Authentication based on gait typically uses a sequence of images of a walking person.

Humans are quite adept at recognizing a person at a distance from his gait. Although, the characteristic gait of a human walk has been well researched in biomechanics community to detect abnormalities in lower extremity joints, the use of gait for identification purposes is very recent. Typically, gait features are derived from an analysis of video-sequence footage of a walking person and consist of characterization of several different movements of each articulate joint. Currently, there do not exist any commercial systems for performing gait-based authentication. The method of input acquisition for gait is not different from that of acquiring facial pictures, and hence gait may be an acceptable biometric. Since gait determination involves processing of video, it is compute and input intensive.

1.4.8 KEYSTROKE DYNAMICS

It is hypothesized that each person types on a keyboard in a characteristic way. This behavioral biometrics is not expected to be unique to each individual but it offers sufficient discriminatory information to permit identity authentication. Keystroke dynamics is a behavioral biometric; for

some individuals, one may expect to observe a large variations from typical typing patterns. The keystrokes of a person using a system could be monitored unobtrusively as that person is keying in other information. Keystroke dynamic features are based on time durations between the keystrokes. Some variants of identity authentication use features based on inter-key delays as well as dwell times - how long a person holds down a key. Typical matching approaches use a neural network architecture to associate identity with the keystroke dynamics features. Some commercial systems are already appearing in the market.

1.4.9 DNA

DNA (Deoxyribonucleic Acid) is the one-dimensional ultimate unique code for one's individuality - except for the fact that identical twins have the identical DNA pattern(Figure 1.9) . It is, however, currently used mostly in the context of forensic applications for identification .
Three issues limit the utility of this biometrics for other applications:

(i) Contamination and sensitivity: it is easy to steal a piece of DNA from an unsuspecting subject to be subsequently abused for an ulterior purpose;

(ii) Automatic real-time identification issues: the present technology for genetic matching is not geared for online unobtrusive identifications. Most of the human DNA is identical for the entire human species and only some relatively small number of specific locations (polymorphic loci) on DNA exhibit individual variation. These variations are manifested either in the number of repetitions of a block of base sequence (length polymorphism) or in the minor non-functional perturbations of the base sequence (sequence polymorphism) .

Figure 1.9 DNA is double helix structure made of four bases:
Adenine (A), Thymine(T), Cytosine (C), and Guanine (G

The processes involved in DNA based personal identification determine whether two DNA samples originate from the same/different individual(s) based on the distinctive signature at one or more polymorphic loci. A major component of these processes now exist in the form of cumbersome chemical methods (wet processes) requiring an expert's skills. There does not seem to be any effort directed at a complete automation of all the processes.

(iii) Privacy issues: information about susceptibilities of a person to certain diseases could be gained from the DNA pattern and there is a concern that the unintended abuse of genetic code information may result in discrimination in e.g., hiring practices.

1.4.10 SIGNATURE AND ACOUSTIC EMISSIONS

The way a person signs her name is known to be a characteristic of that individual Although signatures require contact and effort with the writing instrument, they seem to be acceptable in many government, legal, and The way a person signs her name is known to be a characteristic of that individual (Figure 1.10) .Although signatures require contact and effort with the writing instrument, they seem to be acceptable in many government, legal, and commercial transactions4 as a method of personal authentication. Signatures are a behavioral biometric, evolve over a period of time and are influenced by physical and emotional conditions of the signatories. Signatures of some people vary a lot: even the successive impressions of their signature are significantly different. Further, the professional forgers can reproduce signatures to fool the unskilled eye. Although, the human experts can discriminate genuine signatures from the forged ones, modeling the invariance in the signatures and automating signature recognition process are challenging. There are two approaches to signature verification: static and dynamic. In static signature verification, only geometric (shape) features of the signature are used for authenticating an identity . Typically, the signature impressions are normalized to a known size and decomposed into simple components (strokes). The shapes and relationships of strokes are used as features. In dynamic signature verification, not only the shape features are used for authenticating the signature but the dynamic features like
acceleration, velocity, and trajectory profiles of the signature are also employed. The signature impressions are processed as in a static signature verification system. Invariants of the dynamic features augment the static features, making forgery difficult since the forger has to not only know the impression of the signature but also the way the impression was made. A related

technology is authentication of an identity based on the characteristics of the acoustic emissions emitted during a signature scribble. These acoustic emissions are claimed to be a characteristic of each individual .

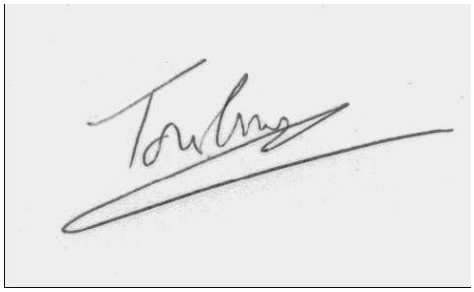


Figure1. 10 Identification based on signature.

1.4.11 ODOR

It is known that each object exudes an odor that is characteristic of its chemical composition and could be used for distinguishing various objects. Among other things, the automatic odor detection technology is presently being 4 In some developing countries with low literacy rates, “thumbprint” is accepted as a legal signature. It is known that each object exudes an odor that is characteristic of its chemical composition and could be used for distinguishing various objects. Among other things, the automatic odor detection technology is presently being investigated for detecting land mines . A whiff of air surrounding an object is blown over an array of chemical sensors, each sensitive to a certain group of (aromatic) compounds. The feature vector consists of the signature comprising of the normalized measurements from each sensor. After each act of sensing, the sensors need to be initialized by a flux of clean air. Body odor serves several functions including communication, attracting mates, assertion of territorial rights, and protection from a predator. A component of the odor emitted by a human (or any animal) body is distinctive to a particular individual. It is not clear if the invariance in a body odor could be detected despite deodorant smells, and varying chemical composition of the surrounding environment. Currently, no commercial odor based identity authentication systems exist.

1.4.12 RETINAL SCAN

The retinal vasculature is rich in structure and is supposed to be a characteristic of each individual and each eye. It is claimed to be the most secure biometrics since it is not easy to change or replicate the retinal vasculature. Retinal scans(Figure 1.11), glamorized in movies and military installations, are mostly responsible for the “high-tech-expensive” impression of the biometric technology5. The image capture requires a person to peep into an eye-piece and focus on a specific spot in the visual field so that a predetermined part of the retinal vasculature could be imaged. The image acquisition involves cooperation of the subject, entails contact with the eyepiece, and requires a conscious effort on the part of the user. All these factors adversely affect the public acceptability of retinal biometric. A number of retinal scan-based identity authentication installations are in operation which boasts *zero* false positives in all the installations to-date6. Retinal vasculature can reveal some medical conditions, e.g., hypertension, which is another factor standing in the way of public acceptance of retinal scan based-biometrics.

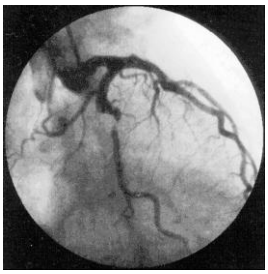


Figure1. 11 Authentication based on Retinal Scan.

1.4.13 HAND AND FINGER GEOMETRY

In recent years, hand geometry has become a very popular access control biometrics which has captured almost half of the physical access control market . Some features related to a human hand, e.g., length of fingers, are relatively invariant and peculiar (although, not unique) to each individual. The image acquisition system requires cooperation of the subject and captures frontal and side view images of the palm flatly placed on a panel with outstretched fingers. The registration of the palm is accomplished by requiring the subject's fingers to be aligned with a system of pegs on the panel which is not convenient for subjects with limited flexibility of palm,

e.g., those suffering from arthritis. The representational requirements of the hand are very small (9 bytes) which is

an attractive feature for bandwidth and memory limited systems. The hand geometry is not unique and cannot be scaled up for systems requiring identification of an individual from a large population of identities. In spite of this, hand geometry has gained acceptability in a number of the installations in last few years for identity authentication applications. Finger geometry is a variant of hand geometry and is a relatively new technology which relies only on geometrical invariants of fingers (index and middle). A finger geometry acquisition device closely resembles that for hand geometry but is more compact. It is claimed to be more accurate than hand geometry. However, the technology for finger geometry based authentication is not as mature as that for hand geometry.

1.5 CHALLENGES IN DESIGN OF SYSTEM

It is not clear whether the use of the features and philosophies underlying the identification systems heavily tuned for human use (e.g., faces and fingerprints) is as effective for fully automatic processes. Neither is it know whether identification technologies inspired and used by humans are indeed as amenable and effective for completely automatic identification systems. In fact, it is not even clear if the solutions solely relying on biometrics-based identifications are the most desirable engineering solutions in many real-world applications. Both, a different set of functional requirements demanded by the emerging market applications and the retrospective wisdom of futility of myopic dependence on human intuition for engineering designs suggest that full automation of the biometrics-based identification systems warrant a careful examination of all the underlying components of the positive identifications of the emerging applications[1].

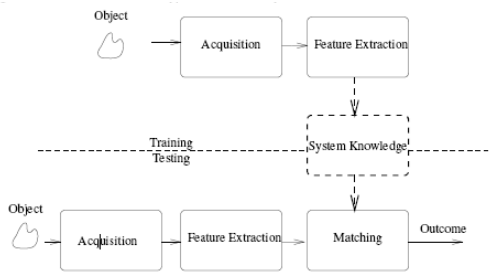


Fig 1.12 A Typical Automated Biometric Identification System

During enrollment, biometric measurements are captured from a given subject, relevant information from the raw measurement is gleaned by the feature extractor, and (feature, person) information is stored in a database. Additionally, some form of ID for the subject may be generated for the subject (along with the visual/machine representation of the biometrics). In identification mode, the system senses the biometric measurements from the subject, extracts features from the raw measurements, and searches the database using the features thus extracted. The system may either be able to determine the identity of the subject or decide the person is not represented in the database. In authentication mode of operation, the subject presents his system assigned ID and the biometric measurements, the system extracts (input) features from the measurements, and attempts to match the input features to the (template) features corresponding to subject's ID in the system database. The system may, then, either determine that the subject is who he claims to be or may reject the claim. In some situations, a single system operates as both an identification and an authentication system with a common database of (identity, feature) associations.

Described below are some of the research problems in the design of biometrics-based identification systems.

1. Acquisition. Acquiring relevant data for the biometrics is one of the critical processes which has not received adequate attention. The amount of care taken in acquiring the data (often) determines the performance of the entire system. Two of the associated tasks are:

a. Quality assessment: Automatically assessing the suitability of the input data for automatic processing and
b. Segmentation :Separation of the input data into foreground (object of interest) and background (irrelevant information). A number of opportunities exist for incorporating the context of the data capture which may further help improve the performance of the system and avoiding undesirable measurements (and subsequent recapture of desirable measurements).

With inexpensive desktop computing and large input bandwidth, typically the context of the data capture could be made richer to improve the performance. For instance, a fingerprint is traditionally captured from its 2D projection on a flat surface. Why not capture a 3D image? Why not take a color image? Why not use active sensing? Such enhancements may often improve

the performance of the biometric systems. Although a number of existing identification systems routinely assign a quality index to the input measurement indicating its desirability for matching ,the approach to such a quality assessment metric is subjective, debatable, and typically inconsistent. A lot of research effort needs to be focused in this area to systematize both

- The rigorous and realistic models of the input measurements and
- Metrics for assessment of quality of a measurement.

When the choice of rejecting a poor quality input measurement is not available (e.g., in legacy databases), the system may optionally attempt at gleaning useful signal from the noisy input measurements. Such operation is referred to as signal/image enhancement and is computationally intensive. How to enhance the input measurements without introducing any artifacts is an active research topic. Similarly, the conventional foreground/background separation typically relies on an ad hoc processing of input measurements and enhancing the information bandwidth of input channel (e.g., using more sensory channels) often provides very effective avenues for segmentation. Further, robust and realistic models of the object of interest often facilitate cleaner and better design of segmentation algorithms.

2. Representation : To detect the machine-readable representations completely capture the invariant and discriminatory information in the input measurements is the most challenging problem in representing biometric data. This representation issue constitutes the essence of system design and has far reaching implications on the design of the rest of the system. The unprocessed measurement values are typically not invariant over the time of capture and there is a need to determine salient features of the input measurement which both discriminate between the identities as well as remain invariant for a given individual. Thus, the problem of representation is to determine a measurement (feature) space which is invariant (less variant) for the input signals belonging to the same identity and which differ maximally for those belonging to different identities (high *interclass*) variation and low *interclass* variation). To systematically determine the discriminatory power of an information source and arrive at an effective feature space is a challenging problem. A related issue about representation is the *saliency* of a measurement signal and its representation. More distinctive biometric signals offer more reliable identity authentication. Less complex measurement signals inherently offer a less reliable identification. This phenomenon has a direct impact in many biometrics-based identification, e.g., signature, where less distinctive signatures could be easily forged. A systematic method of quantifying distinctiveness of a specific signal associated with an identity and its representation is needed for effective identification systems. Additionally, in some

applications, storage space is at a premium, e.g., in a smart card application, typically, about 2K bytes of storage is available. In such situations, the representation also needs to be parsimonious. The issues of most salient features of an information source also need to be investigated. Representation issues cannot be completely resolved independent of a specific biometric domain and involve complex trade-offs. Take, for instance, the fingerprint domain. Representations based on the entire gray scale profile of a fingerprint image are prevalent among the verification systems using optical matching. However, the utility of the systems using such representation schemes may be limited due to factors like brightness variations, image quality variations, scars, and large global distortions present in the fingerprint image because these systems are essentially resorting to template matching strategies for verification. Further, in many verification applications terser representations are desirable which preclude representations that involve the entire gray scale profile of fingerprint images. Some system designers attempt to circumvent this problem by restricting that the representation be derived from a *small* (but consistent) part of the finger . However, if this same representation is also being used for identification applications, then the resulting systems might stand at a risk of restricting the number of unique identities that could be handled, simply because of the fact that the number of distinguishable templates is limited. On the other hand, an image-based representation makes fewer assumptions about the application domain (fingerprints) and, therefore, has the potential to be robust to wider varieties of fingerprint images. For instance, it is extremely difficult to extract a landmark-based representation from a (degenerate) finger devoid of any ridge structure.

3. Feature Extraction: Given raw input measurements, automatically extracting the given representation is an extremely difficult problem, especially where input measurements are noisy. The figure below(Figure 1.13) shows an automated Finger Print Identification system.

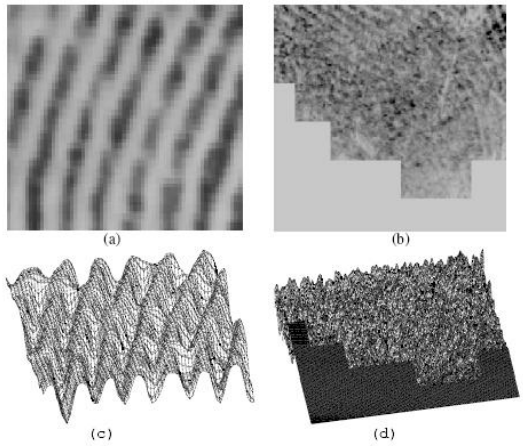


Figure 1.13 Automatically gleaning finger features from the fingerprint images is extremely difficult, especially, when the fingerprint is of poor quality (a) a portion of good quality fingerprint image; (b) a portion of poor quality fingerprint image; (c) 3-dimensional visualization of (a); and (d) 3-dimensional visualization of (b).

A given arbitrarily complex representation scheme should be amenable to automation without any human intervention. For instance, the manual system of fingerprint identification uses as much as a dozen features . However, it is not feasible to incorporate these features into a fully automatic fingerprint system because it not easy to reliably detect these features using state-of-the-art image processing techniques. Determining features that are amenable to automation has not received much attention in computer vision and pattern recognition research and is especially important in biometrics which are entrenched in the design philosophies of an associated mature manual system of identification. Traditionally, the feature extraction system follows a staged sequential architecture which precludes effective integration of extracted information available from the measurements. Increased availability of inexpensive computing and sensing resources makes it possible to use better architectures/methods for information processing to detect the features reliably. Once the features are determined, it is also a common practice to design feature extraction process in a somewhat ad hoc manner. The efficacy of such methods is limited especially when input measurements are noisy. Rigorous models of feature representations are helpful in a reliable extraction of the features from the input measurements, especially, in noisy situations. Determining terse and effective models for the features is a challenging research problem.

4. Matching: The crux of a matcher is a similarity function which quantifies the intuition of similarity between two representations of the biometric measurements. Determining an

appropriate similarity metric is a very difficult problem since it should be able to discriminate between the representations of two different identities despite noise, structural and statistical variations in the input signals, aging, and artifacts of the feature extraction module. In many biometrics, say signature verification, it is difficult to even define the ground truth : do the given two signatures belong to the same person or different persons? A representation scheme and a similarity metric determine the accuracy performance of the system for a given population of identities; hence the selection of appropriate similarity scheme and representation is critical. Given a complex operating environment, it is critical to identify a set of valid assumptions upon which the matcher design could be based. Often, there is a choice between whether it is more effective to exert more constraints by incorporating better engineering design or to build a more sophisticated similarity function for the given representation. For instance, in a fingerprint matcher(Figure 1.14), one could constrain the elastic distortion altogether and design the matcher based on a rigid transformation assumption or allow arbitrary distortions and accommodate the variations in the input signals using a clever matcher. Where to strike the compromise between the complexity of the matcher and controlling the environment is an open problem.

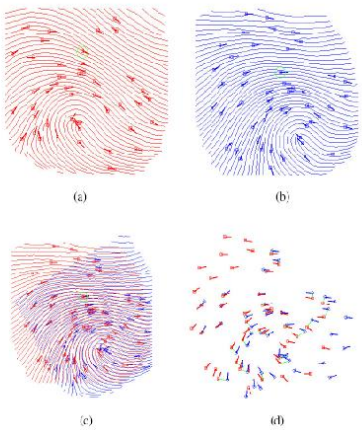


Figure 1.14 Fingerprint Matcher: Results of applying the matching algorithm to an input and a template minutiae set; (a) input minutiae set; (b) template minutiae set; (c)input and template fingerprint are aligned based on the minutiae marked with green circles; and (d) matching result where template minutiae and their correspondences are connected by green lines. The matching score for the fingerprints was 37. The score range was 0--100; scores closer to 100 indicate better match.

Typically, the fingerprint imaging system presents a number of peculiar and challenging situations some of which are unique to fingerprint image capture scenario:

i. Inconsistent contact: the act of sensing distorts the finger. The three-dimensional shape of the finger gets mapped onto the two-dimensional surface of the glass platen.

Typically, this (non homogeneous) mapping function is determined by the pressure and contact of the finger on the glass platen .

ii. Non-uniform contact: the ridge structure of a finger would be completely captured if ridges of the part of the finger being imaged are in complete optical contact with the glass platen. However, the dryness of the skin, skin disease, sweat, dirt, humidity in the air all confound the situation resulting in a non-ideal contact situation: some parts of the ridges may not come in complete contact with the platen and regions representing some valleys may come in contact with the glass platen. This results in “noisy” low contrast images, leading to either spurious minutiae or missing minutiae.

iii. Irreproducible contact: vigorous manual work, accidents etc. inflict injuries to the finger, thereby, changing the ridge structure of the finger either permanently or semi-permanently. This may introduce additional spurious minutiae.

iv. Feature extraction artifacts: the feature extraction algorithm is imperfect and introduces measurement errors. Various image processing operations might introduce inconsistent biases to perturb the location and orientation estimates of the reported minutiae from their gray scale counterparts.

The act of sensing itself adds noise to the image. For example, residues are leftover on the glass platen from the previous fingerprint capture. A typical imaging system distorts the image of the object being sensed due to imperfect imaging conditions. In the frustrated total internal reflection (FTIR) sensing scheme, for example, there is a geometric distortion because the image plane is not parallel to the glass platen.

5. Search, organization, and scalability: systems dealing with a large number of identities should be able to effectively operate as the number of users in the system increases to its operational capacity and should only gracefully degrade as the system accommodates more users than envisaged at the time of its design. As civilian applications (e.g., driver and voter registration, National ID systems and IDs for health, medical, banking, cellular, transportation, and e-commerce applications) enrolling a very large number of identities (e.g., tens of millions) are being designed and integrated, we are increasingly looking toward biometrics to solve authentication and identification problems. In identity authentication systems, biometrics are cost effective and are easier

to maintain because these systems do not have to critically depend on issuing/reissuing other identity (magnetic stripe/smart/2D bar code) cards. Tasks like maintaining the database of identities, selection of a record etc. may require more resources, but the technical complexity of

matching a biometric representation offered by the user to that stored in the system does not increase as the number of identities handled by the system increases arbitrarily. On the other hand, identification of an individual among a large number of identities becomes increasingly complex as the number of identities stored in the system increases. Many applications like National ID systems, passport and visa issuance further require a constant throughput and a very small turnaround time. A designer of such systems needs to adopt radically different strategies and mode of operation than those adopted by traditional forensic identification systems. This has a profound influence on every aspect of the system, including the choice of biometrics, features, metric of similarity, matching criteria, operating point, etc. None of these design issues have been rigorously studied, neither in biometrics nor even in pattern recognition research. All these criteria point to using those biometrics which remain invariant over a long period of time. Designing constant length, one-dimensional, indexable features will become increasingly important for identification applications involving a large number of identities.

1.6 EVALUATION OF A BIOMETRIC SYSTEM

The following parameters are gene3rally used to measure the efficiency of a biometric system:

- **False Acceptance Rate (FAR)**

The FAR is the frequency that a non authorized person is accepted as authorized. Because a false acceptance can often lead to damages, FAR is generally a security relevant measure. FAR is a non-stationary statistical quantity which does not only show a personal correlation, it can even be determined for each individual biometric characteristic (called personal FAR).

- **False Rejection Rate (FRR)**

The FRR is the frequency that an authorized person is rejected access. FRR is generally thought of as a comfort criteria, because a false rejection is most of all annoying. FRR is a non-stationary statistical quantity which does not only show a strong personal correlation, it can even be determined for each individual biometric characteristic (called personal FRR).

- **Failure To Enroll rate (FTE, also FER)**

The FER is the proportion of people who fail to be enroled successfully. FER is a non-stationary statistical quantity which does not only show a strong personal correlation, it can even be determined for each individual biometric characteristic (called personalFER). Those who are enroled yet but are mistakenly rejected after many verification/identification attempts count for the Failure To Acquire (FTA) rate. FTA can originate through temporarily not

measurable features ("bandage", non-sufficient sensor image quality, etc.). The FTA usually is considered within the FRR and need not be calculated separately, see also FNMR and FMR.

- **False Identification Rate (FIR)**

The False Identification Rate is the probability in an identification that the biometric features are falsely assigned to a reference. The exact definition depends on the assignment strategy; namely, after feature comparison, often more than one reference will exceed the decision threshold.

1.6.1 FRR IN DETAIL

Due to the statistical nature of the false rejection rate, a large number of verification attempts have to be undertaken to get statistical reliable results. The verification can be successful or unsuccessful. In determining the FRR, only fingerprints from successfully enrolled users are considered. The probability for lack of success (FRR(n)) for a certain person is measured:

$$FRR(n) = \frac{\text{Number of rejected verification attempts for a qualified person (or feature) n}}{\text{Number of all verification attempts for a qualified person (or feature) n}}$$

These values are better with more independent attempts per person/feature. The overall FRR for N participants is defined as the average of FRR(n):

$$FRR = \frac{1}{N} \sum_{n=1}^{N} FRR(n) \qquad (1.1)$$

The values are more accurate with higher numbers of participants (N). Alternatively, the median value may be calculated.

Important: the determined FRR includes both poor picture quality and other rejection reasons such as finger position, rotation, etc. in the reasons for rejection. In many systems, however, rejections due to bad quality are generally independent of the threshold. The FRR after quality filtering is similarly defined:

$$\frac{\text{Number of rejected "qualified" attempts}}{\text{Total number of "qualified" attempts}} \qquad (1.2)$$

An FRR defined as such, generally yields better data sheet values, but these lower numbers are not reflected in reality from a user's perspective.
Finally, the result of a verification attempt has to be defined exactly:
A verification attempt is *successful* if the user interface of the application provides a "successful" message or if the desired access is granted.
A verification attempt counts as *rejected* if the user interface of the application provides an "unsuccessful" message.
In cases of no reaction, a verification time interval has to be given to ensure comparability. If the time interval has expired the verification attempt is counted *unsuccessful*.

1.6.2FAR IN DETAIL

Due to the statistical nature of the false acceptance rate, a large number of fraud attempts have to be undertaken to get statistical reliable results. The fraud trial can be successful or unsuccessful. The probability for success (FAR(n)) against a certain enroled person n is measured:

$$FAR(n) = \frac{\text{Number of successful independent fraud attempts against a person (or characteristic) n}}{\text{Number of all independent fraud attempts against a person (or characteristic) n}} \qquad (1.3)$$

These values are more reliable with more independent attempts per person/characteristic. In this context, independency means that all fraud attempts have to be performed with different persons or characteristics! The overall FAR for N participants is defined as the average of all FAR(n):

$$FAR = \frac{1}{N} \sum FAR(n)$$

$$\sum_{n=1}^{N}$$

(1.4)

The values are more accurate with higher numbers of different participants/characteristics (N). Alternatively, the median value may be calculated.

The crucial number for the determination of statistic significance is the number of *independent* attempts. Obviously, two attempts in which alternately one person is the reference and another places the request, are not independent of each other. Likewise, multiple attempts from one unauthorized user are considered dependent and therefore have less meaning for statistical significance.

Finally, the following items have to be settled, or defined, respectively:

- What is a fraud attempt?
- How is the result of a fraud attempt defined exactly?

Usually, during FAR determination, a fraud attempt is an attack using the characteristics of non-authorized persons. This, however, pretends a high security which may not be present since there are a lot of further possibilities for promising attacks.

- A fraud attempt is *successful* if the user interface of the application provides a "successful" message or if the desired access is granted.
- A fraud attempt counts as *rejected* if the user interface of the application provides an "unsuccessful" message.
- In cases where no "unsuccessful" message is available, a verification time interval has to be given to ensure comparability. If the verification time interval has expired the fraud attempt is counted *unsuccessful*.

1.6.3 HOW DO THE FAR/FRR PAIRED GRAPHS AFFECT A BIOMETRIC SYSTEM

The error graphs of FAR and FRR are respectively defined as the probability that an unauthorized user is accepted as authorized, and that an authorized user is rejected as unauthorized. The curves are dependent upon an adjustable decision threshold for the similarity of a scanned biometric characteristic to a saved reference. The following derivations

apply under the assumption that a similarity rating value can be any whole number between 0 and K, and that, for simplicity's sake, the probability of value K occurring is 0. It also makes sense in practical applications, when we first consider the FMR and the FNMR and later extract the threshold-independent rejections due to insufficient image quality from the FAR and FRR. Furthermore, we assume that for acceptance the coincidence of two features and for rejection the non-coincidence is required.

If a general probability distribution function p is given for discrete similarity values n, the probability $P_M(th)$ that the scanned biometric characteristic with similarity rating n falls below threshold th ("misses") is:

$$P_M(0) := 0$$

$$P_M(th) = \sum_{n=0}^{th-1} p(n) \quad th = 1, 2, 3, ..., K \qquad (1.5)$$

The sum of correct matches and mismatches must equal the number of total events. For that reason, the probability $P_H(th)$ that the similarity rating of the scanned trait reaches or exceeds threshold th ("hits") will be

$$P_H(th) = 1 - P_M(th) = \sum_{n=th}^{K} p(n) \quad th = 0, 1, 2, ..., K \qquad (1.6)$$

The False Match Rate FMR(th) is an estimation to the probability that the similarity of two non-identical features does not reach or exceed a certain threshold value th. Therefore:

$$FMR(th) \sim P_H(th) = 1 - \sum_{n=0}^{th-1} p_N(n) \quad th = 1, 2, 3, ..., K \qquad (1.7)$$

For the False Non-Match Rate FNMR (th), applies the analogous:

$$FNMR(th) \sim P_M(th) = \sum_{n=0}^{th-1} p_B(n) \quad th = 1, 2, 3, ..., K \qquad (1.8)$$

where p_N is the probability frequency function for non authorized users and p_B is for authorized users. The approximation (~) indicates that only the *expected value* of the measured failure rates FMR and FNMR are identical with the probabilities P_H resp. P_M. The limit values are:

$$FMR(0) = 1 \qquad FMR(K) = 0$$

$$FNMR(0) = 0 \qquad FNMR(K) = 1$$

To calculate FAR and FRR, the threshold-independent quality rejection rate QRR (equals FTA, depending on definition) has to be taken into consideration. Provided that a false acceptance is assigned to a false match, we obtain:

$$FAR(th) = (1 - QRR)\ FMR(th)$$

$$FRR(th) = QRR + (1 - QRR)\ FNMR(th)$$

For the border values we then get:

$$FAR(0) = 1 - QRR \qquad FAR(K) = 0$$

$$FRR(0) = QRR \qquad FRR(K) = 1$$

Setting a similarity rating th as the threshold to differentiate between authorized and non authorized users, results in the experimental estimation of false acceptance rate FAR(th), as the number of similarity ratings of non authorized users that fall above this threshold in comparison to all trials / number of similarity ratings. Conversely, the false rejection rate FRR is the number of authorized user's similarity ratings which fall below this same threshold compared with the total inquiries. Through integration (in practice, successive summation) of the probability distribution curves, FAR and FRR graphs are determined, which are dependent on the

adjustable adopted threshold th. The following diagrams show typical results in linear and logarithmic scale:

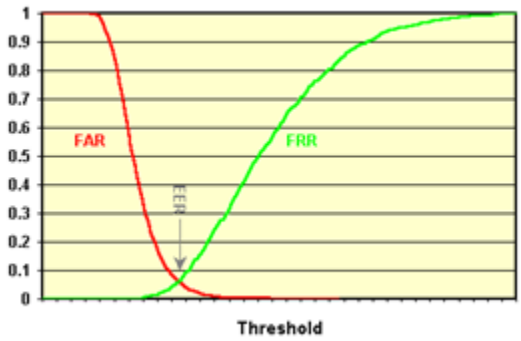


Figure 1.15 FAR Diagram

1.6.4 RECIEVER OPERATING CHARACTERISTIC (ROC) of a BIOMETRIC SYSTEM

The FAR/FRR curve pair is excellently suited to set an optimal threshold for the biometric system. Further predictors of a system's performance, however, are limited. This is partially due to the interpretation of the threshold and similarity measures. The definition of the similarity measures is a question of implementation. Almost arbitrary scaling and transformations are possible, which affect the appearance of FAR/FRR curves but not the FAR-FRR values at a certain threshold. A popular example is the use of a "distance measure" between the biometric reference and the scanned biometric features. The greater the similarity, the smaller the distance. The result is a mirror image of the FAR/FRR curves. A favorite trick is to stretch the scale of FAR/FRR curves near the EER (Equal Error Rate: FAR(th) = FRR(th)), (i.e., using more threshold values) thus making the system appear less sensitive to threshold changes.

In order to reach an effective comparison of different systems, a description independent of threshold scaling is required. One such example from the radar technology is the *Receiver Operating Characteristic (ROC),* which plots FRR values directly against FAR values, thereby eliminating threshold parameters. The ROC, like the FRR, can only take on values between 0 and 1 and is limited to values between 0 and 1 on the x axis (FAR). It has the following characteristics:

- The ideal ROC only have values that lie either on the x axis (FAR) or the y axis (FRR); i.e., when the FRR is not 0, the FAR is 1, or vice versa.

- The highest point (linear scale under the definitions used here) is for all systems given by FAR=0 and FRR=1.
- The ROC cannot increase

As the ROC curves for good systems lie very near the coordinate axis, it is reasonable for one or both axis to use a logarithmic scale:

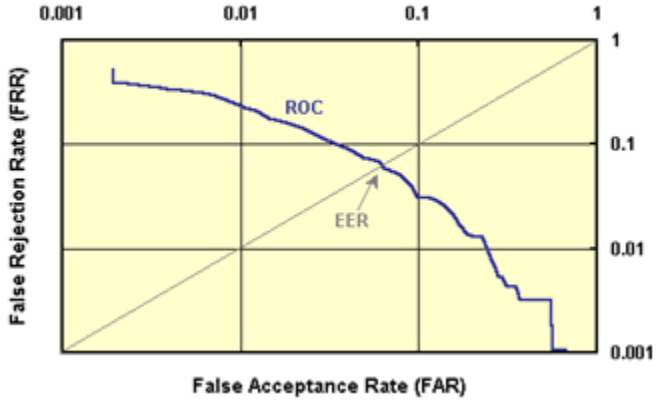


Figure 1.16 ROC Curve for a Biometric System

Instead of "ROC", sometimes the term "DET" (Detection Error Tradeoff) is used. In those cases, the term "ROC" is reserved for the complimentary plot 1 - FRR against FAR

CHAPTER 2

FEATURE LEVEL CLUSTERING OF LARGE BIOMETRIC DATABASES

2.1 INTRODUCTION

Existence of a large number of biometric records in the database requires rapid and efficient searching method. With the increase in the size of the biometric database, reliability and scalability issues become the bottleneck for low response time, high search and retrieval efficiency in addition to accuracy. Traditionally identification systems claims identity of an individual by searching templates of all users enrolled in the database . These comparisons increase the data retrieval time along with the error rates. Thus a size reduction technique must be applied to reduce the search space and thus improve the efficiency. Conventionally databases are indexed numerically or alphabetically to increase the efficiency of retrieval. However, biometric databases do not posses a natural order of arrangement which negates the idea to index them alphabetically/numerically. Reduction of search space in biometric databases thus remains a challenging problem. To reduce search space certain classification, clustering and indexing approaches have been proposed. In supervised classification or discriminant analysis, a collection of labeled (pre-classified) patterns are provided; the problem is to label a newly encountered, yet unlabeled, pattern. Typically, the given labeled (training) patterns are used to learn the descriptions of classes which in turn are used to label a new pattern. There exist several classification techniques like classification of face images based on age [2] where input images can be classified into one of three age-groups: babies, adults, and senior adults. Gender classification from frontal facial images using genetic feature subset selection is considered in [3]. Most of the existing fingerprint classification approaches make use of the orientation image [4]. An algorithm for the automatic coarse classification of iris images using box-counting method to estimate the fractal dimensions of iris is given in [5]. The main drawback of classification is that it is the supervised method where number of classes has to be known in advance. Further the data within each class is not uniformly distributed so the time required to search some classes is comparatively large. The limitations of classification can be addressed with unsupervised approach known as *Clustering*. It involves the task of dividing data points into homogeneous classes or clusters so that items in the same class are as similar as possible and items in different classes are as dissimilar as possible [6]. Intuitively it can be visualized as a form of data compression, where a large number of samples are converted into a small number of representative prototypes. Clustering can be broadly classified into Hard and

Fuzzy approaches [7]. Non-fuzzy or hard clustering divides data into crisp clusters, where each data point belongs to exactly one cluster(Figure 2.1). Fuzzy clustering segments the data such that each sample data point can belong to more than one cluster and each data point has some degree of association with every cluster(Figure 2.2). The sum of the membership grades of a particular data point belonging to more than one cluster is always one. From the available biometric features it has been inferred that each feature set has an association with more than one cluster and may have dissimilarity with data of the same cluster. In other words they are said to show inter class similarities and intra class variations, thus making them difficult to assign them to a single cluster. For example, variations in the face image of an individual due to change in pose, expression, lighting and eye glasses. Hence fuzzy clustering techniques prove to be an efficient means for grouping biometric data.

2.2 FUZZY C MEANS

Clustering involves the process of arranging data points in such a way that items sharing similar characteristics are grouped together. The goal is to find the natural grouping of data points without prior knowledge of class labels (unsupervised). Fuzzy C Means (FCM) is a feature clustering technique wherein each feature point belongs to a cluster by some degree that is specified by a membership grade [8]. These kind of clustering algorithms are known as objective function based clustering. Given M dimensional database of size N where N is the total number of feature vectors and M is the dimension of each feature vector. FCM assigns every feature vector a membership grade for each cluster. The problem is to partition the database based on some fuzziness criteria using membership values. To find membership values, the partition matrix U of size $N \times c$ is calculated that defines membership degrees of each feature vector. The values 0 and 1 in U indicate no membership and full membership respectively. Grades between 0 and 1 indicate that the feature point has partial membership in a cluster. Looking at the picture, we may identify two clusters in proximity of the two data concentrations. We will refer to them using ‘A’ and ‘B’. In the first approach shown in this tutorial - the k-means algorithm - we associated each datum to a specific centroid; therefore, this membership function looked like this:

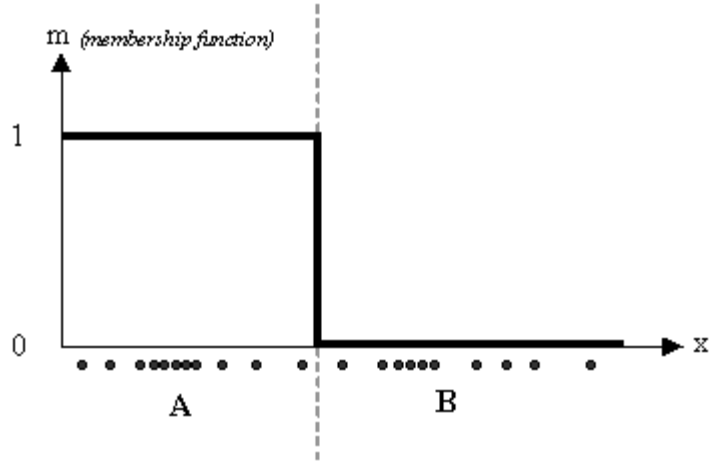


Figure 2.1 Hard or Crisp Clustering of Data

In the FCM approach, instead, the same given datum does not belong exclusively to a well defined cluster, but it can be placed in a middle way.[9] In this case, the membership function follows a smoother line to indicate that every datum may belong to several clusters with different values of the membership coefficient.

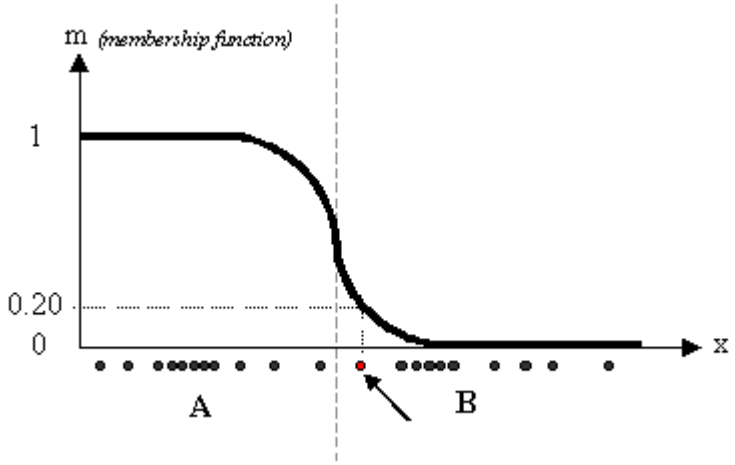


Figure 2.2 Memebershio of Data in Fuzzy Clsutering

In the figure above, the datum shown as a red marked spot belongs more to the B cluster rather than the A cluster. The value 0.2 of ‘m’ indicates the degree of membership to A for such datum. Now, instead of using a graphical representation, we introduce a matrix U whose factors are the ones taken from the membership functions:

$$U_{MC} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ .. & .. \\ 0 & 1 \end{bmatrix} \qquad U_{MC} = \begin{bmatrix} 0.8 & 0.2 \\ 0.3 & 0.7 \\ 0.6 & 0.4 \\ .. & .. \\ 0.9 & 0.1 \end{bmatrix}$$

(a) (b)

The number of rows and columns depends on how many data and clusters we are considering. More exactly we have C = 2 columns (C = 2 clusters) and N rows, where C is the total number of clusters and N is the total number of data. The generic element is so indicated: u_{ij}. In the examples above we have considered the k-means (a) and FCM (b) cases. We can notice that in the first case (a) the coefficients are always unitary. It is so to indicate the fact that each datum can belong only to one cluster. Other properties are shown below:

- $u_{ij} \in [0,1] \qquad \forall i, j$
- $\sum_{j=1}^{C} u_{ik} = 1 \qquad \forall i$
- $0 < \sum_{i=1}^{N} u_{ij} < N \quad \forall N$

The following steps are involved in training the database using FCM technique

2.1 Initialization of the partition matrix

Initially a fuzzy partition matrix *U* is generated that is of size *N*×*c*, where *c* is number of clusters and *N* is total number of feature vectors. Subject to the constraint that

$$\sum_{j=1}^{c} U_{ij} = 1, \qquad \forall i \varepsilon \{1,2,...N\} \tag{2.1}$$

2.2 Calculation of fuzzy centers

The fuzzy centers are calculated using the partition matrix generated in 2.1.

$$C_j = \frac{\sum_{i=1}^{N} U_{ij}^{m} \times x_i}{\sum_{i=1}^{N} U_{ij}^{m}} \tag{2.2}$$

where $m \geq 1$ is a fuzzification exponent. The larger the value of m the fuzzier the solution will be. This indicates the number of iterations that is required for clustering. x_i is i^{th} feature vector. The value of i ranges from 1 to N (total number of templates in the database).

2.3 Updating membership and cluster centers

FCM is an iteration loop. The method of clustering is based on minimization of the objective function defined by

$$J_m = \sum_{i=1}^{N}\sum_{j=1}^{C} U_{ij}^{m} \left\| x_i - c_j \right\|^2 \qquad (2.3)$$

U_{ij} describes the degree of member of feature set (x_i) with cluster c_j. ||*|| represents norm between x_i and cluster center c_j given by

$$\| x_i - c_j \|^2 = (x_i - c_j)^T A (x_i - c_j) \qquad (2.4)$$

where A is identity matrix for Euclidean distance used here. At every iteration the membership matrix is updated using

$$U_{ij} = \frac{1}{\sum_{k=1}^{c} \left(\frac{\left\| x_i - c_j \right\|}{\left\| x_i - c_k \right\|} \right)^{\frac{2}{m-1}}} \qquad (2.5)$$

The revised membership matrix (generated in (5)) is used for updating the cluster centers using equation (2). The iteration will stop when $max_{ij}\{|U_{ij}^{(m+1)} - U_{ij}^{(m)}|\} < \varepsilon$, where ε is a termination criteria. The value of ε ranges between 0 and 1.

The Algorithm for Fuzzy C Means Clustering is as shown in Figure 2.3

Algorithm: *fcmcluster (c: no of clusters, x: input data, N: total number of training data)*

Step 1: Fix $1 \leq m < \infty$, initial partition matrix U^0 (N×c), and the termination criterion ε.

Step 2: Calculate the fuzzy cluster centers c using equation (2).

Step 3: Update membership matrix as per equation (5).

Step 4: Calculate change in membership matrix $\Delta = || U^{m+1} - U^m || = \max_{ij} |U_{ij}^{m+1} - U_{ij}^m|$. If $\Delta > \varepsilon$, then set m=m+1 and go to step 2. If $\Delta \leq \varepsilon$, then stop.

Figure 2.3 Fuzzy C Means Algorithm

2.3 K MEANS ALGORITHM

K-means is one of the simplest unsupervised learning algorithms that solve the well known clustering problem. The procedure follows a simple and easy way to classify a given data set through a certain number of clusters (assume k clusters) fixed a priori. The main idea is to define k centroids, one for each cluster. These centroids should be placed in a cunning way because of different location causes different result. So, the better choice is to place them as much as possible far away from each other. The next step is to take each point belonging to a given data set and associate it to the nearest centroid. When no point is pending, the first step is completed and an early groupage is done. At this point we need to re-calculate k new centroids as barycenters of the clusters resulting from the previous step. After we have these k new centroids, a new binding has to be done between the same data set points and the nearest new centroid. A loop has been generated. As a result of this loop we may notice that the k centroids change their location step by step until no more changes are done. In other words centroids do not move anymore.
Finally, this algorithm aims at minimizing an *objective function*, in this case a squared error function. The objective function

$$J = \sum_{j=1}^{k} \sum_{i=1}^{n} \left\| x_i^{(j)} - c_j \right\|^2 \quad (2.6)$$

,

where $\left\| x_i^{(j)} - c_j \right\|^2$ is a chosen distance measure between a data point $x_i^{(j)}$ and the cluster centre c_j, is an indicator of the distance of the *n* data points from their respective cluster centers.

The algorithm is composed of the following steps:

1. *Place K points into the space represented by the objects that are being clustered. These points represent initial group centroids.*
2. *Assign each object to the group that has the closest centroid.*
3. *When all objects have been assigned, recalculate the positions of the K centroids.*
4. *Repeat Steps 2 and 3 until the centroids no longer move. This produces a separation of the objects into groups from which the metric to be minimized can be calculated.*

Figure 2.4 K Means Algorithm

Although it can be proved that the procedure will always terminate, the k-means algorithm does not necessarily find the most optimal configuration, corresponding to the global objective function minimum. The algorithm is also significantly sensitive to the initial randomly selected cluster centers. The k-means algorithm can be run multiple times to reduce this effect.

K-means is a simple algorithm that has been adapted to many problem domains. As we are going to see, it is a good candidate for extension to work with fuzzy feature vectors.

A Diagrammatic Representation of the Proposed System is given in Figure 2.5

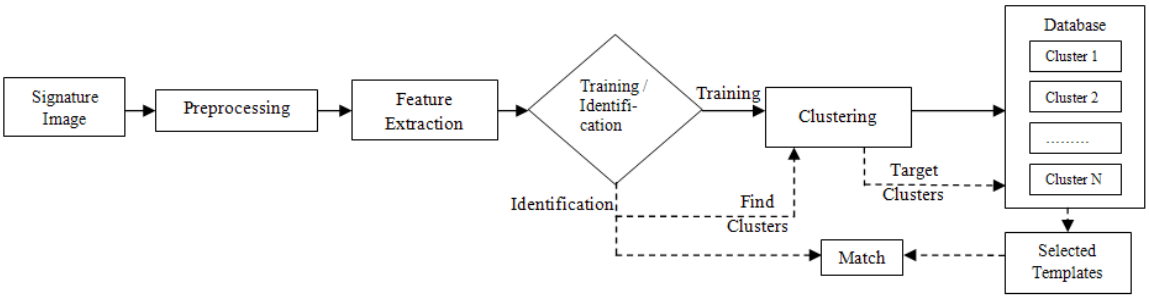


Figure 2.5 Diagrammatic Representation of the Proposed System

As a case study the proposed methodology discussed in this chapter is applied to partition the large biometric database comprising of signature features. The steps involved in clustering the signature database are given in the following section.

2.4 SIGNATURE BIOMETRICS AS A CASE STUDY

2.4.1 Feature extraction and training

Signature is a behavioral characteristic [9] of a person and can be used to identify/verify a person's identity. The signature recognition algorithm consists of two major modules i.e., preprocessing and noise removal and feature extraction. Offline signature acquisition is carried out statically, unlike online signature acquisition, by capturing the signature image using a high resolution scanner. A scanned signature image may require morphological operations like normalization, noise removal by eliminating extra dots from the image, conversion to grayscale, thinning and extraction of high pressure region. The features of the signature images can be classified into two categories: global and local [9].

2.4.1.1 Global features

Global features include the global characteristics of an image. Ismail and Gad [9] have described global features as characteristics which identify or describe the signature as a whole. Examples include: width/height (or length), baseline, area of black pixels etc. They are less responsive to small distortions and hence are less sensitive to noise as well, compared to local features which are confined to a limited portion of the signature.

2.4.1.2 Local features

Local features in contrast to global features are susceptible to small distortions like dirt but are not influenced by other regions of the signature. Hence, though extraction of local features requires a huge number of computations, they are much more precise. However, the grid size has to be chosen very carefully. It can neither be too gross nor too detailed. Examples include local gradients, pixel distribution in local segments etc. Many of the global features such as global baseline, center of gravity, and distribution of black pixels have their local counterparts as well. The features obtained from an input signature image are listed as follows:

1. Width to height ratio
2. Center of gravity (both X and Y coordinates) to height ratio
3. Normalized area of black pixels
4. Total number of components of the signature
5. Global Baseline to height ratio
6. Upper extension to height ratio
7. Lower extension to height ratio.
8. Center of gravity (both X and Y coordinates) of the HPR image to height ratio
9. Area of black pixels in the HPR image to total area of black pixels in the image.
10. Number of cross points to area of black pixels in the thinned image
11. Number of edge points to area of black pixels in the thinned image
12. Slope of the thinned image
13. Trace to area of black pixels in the thinned image

14 to 27. Ratio of centre of gravity co-ordinates to height, ratio of pixel count of individual sections to total pixel count of the image and ratio of baseline position to height of the image in the 3 horizontal sections.

The feature set comprises of

$$F_i = [\, f_1 \; f_2 \ldots\ldots\ldots \; f_{27} \,] \tag{2.7}$$

where *i* ranges from 1 to *N* (total number of templates in the database). The features extracted are used for partitioning the database using FCM clustering technique given in Section 2.2. At

the time of training each data item (F_i with 27 values) is used to find the membership grade with every cluster centre. Data is assigned to cluster with highest value of membership.

2.4.2 Identification strategy

We propose a novel identification strategy for clusters partitioned using fuzzy c means. The identification technique takes into consideration the membership matrix and finds the nearest cluster. Given a query data $q=[q_1\ q_2\ q_3 \ldots q_M]$ the approach updates the membership matrix using exponential modification. Further the Euclidean distance between the j^{th} cluster centre c and query data q is obtained using

$$dist(j) = \sqrt{(q - c_j)^2} \tag{2.8}$$

After obtaining the distance with each cluster centre the objective function is calculated as given in equation (2.3) using initial membership matrix. The membership matrix is updated using calculated distance values (equation (2.8)) as given in equation (2.5). The updated membership matrix is checked for termination criteria against ε. If criteria is met the iteration stops. The fuzzy factor is brought into consideration by choosing clusters with two maximum values of membership grades. The retrieved clusters are chosen to be target clusters to find suitable matches for a particular query signature. The selected templates (K) corresponding to the target cluster ($K \subseteq N$) are retrieved from the database and compared to query template to find a match. The system diagram of proposed identification technique is shown in Figure 2.5. This technique is a preferred over hard clustering techniques as more than one cluster is taken into consideration to declare the identity of an individual. The algorithm for identification is given as given below:

Algorithm: *identify (q: query data, c: cluster centres)*

Step 1: Calculate distance dist between q and c. Initialize the partition matrix U^m.

Step 2: Update the partition matrix U^{m+1} by using dist and U^m.

Step 3: Calculate change in partition matrix $\Delta = || U^{m+1} - U^m || = \max_{ij} | U_{ij}^{m+1} - U_{ij}^m$. If $\Delta > \varepsilon$, then set m = m + 1 and go to step 2. If $\Delta \leq \varepsilon$, then stop.

Step 4: Find two max$\{U^{m+1}\}$ and retrieve target clusters.

2.5 CONCLUSION

We propose an efficient approach to partition the large bio-metric database, to reduce data

retrieval time during identification. The limitations of hard clustering techniques have been removed by introducing the fuzziness criteria. Here fuzziness factor is essential owing to the nature of biometric database. The system is performing comparatively superior as compared to traditional K-Means clustering technique. For less number of clusters the approach is not suitable. However as the size of database increases the number of clusters required for partitioning also increases. Thus it is a preferred partitioning technique for large scale biometric systems. There is still scope of research to find optimum number of clusters that can give maximum accuracy with reduced size of search space for the matcher

CHAPTER 3 DWT BASED HASH CODED EAR BIOMETRIC SYSTEM

3.1 INTRODUCTION

Is this the person who he or she claims to be? Nowadays this question arises incessantly. In different organizations like financial services, e-commerce, telecommunication, government, traffic, health care the security issues are more and more important. It is important to verify that people are allowed to pass some points or use some resources. The security issues are arisen quickly after some crude abuses. For these reason, organizations are interested in taking automated identity authentication systems, which will improve customer satisfaction and operating efficiency. The authentication systems will also save costs and be more accurate that a human being.

Using ear in person identification has been interesting at least 100 years. However, there's no clear evidence that ears are unique. The ear structure is quite complex (Figure 3.1), but the question is, if it is unique for all individuals. At present ear recognition technology has been developed from the initial feasible research to the stage of how to enhance ear recognition performance further, for instance, 3D ear recognition [10], [11], ear recognition with occlusion [12], and multi-pose ear recognition etc. Multi-pose ear recognition is referred to when the angle between the ear and the camera changes, the shape of the ear will be distorted, resulting in the decrease of the recognition performance. Therefore it is necessary to discuss this problem deeply for many researchers. Methods using ear geometrical features which are extracted for ear recognition were easily influenced by pose variations, and evidently are not feasible for human ear recognition with varying poses [13], [14], [15], [16], [17]. Principal component analysis (PCA) was used for ear recognition [18]. However, when data points are distributed in a nonlinear way such as pose variations, PCA fails to discover the nonlinearity hidden in data points. Kernel principal component analysis (KPCA) [19] was also used for ear recognition, but projection results aren't visual using KPCA, and the performance of this method is greatly influenced by kernel parameters. The issue with existing approaches is that they are computationally more expensive in terms of time and space complexity. Thus to have a more robust and efficient biometric system, a novel image hashing technique is proposed for ear biometrics. The system performs well under change in pose, illumination and other transformations.

3.2 EAR BIOMETRICS AS A CASE STUDY

An anthropometric technique of identification based upon ear biometrics was developed by Iannarelli [20]. The “Iannarelli System” is based upon the 12 measurements is shown below.

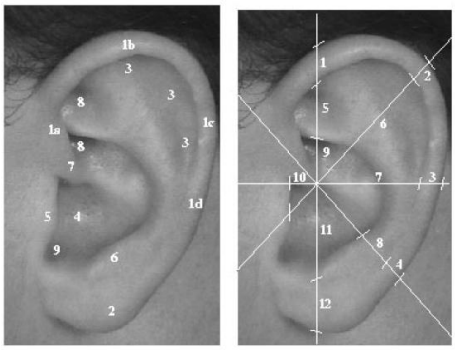


Figure 3.1 Iannarelli System for Ear Biometrics

The locations shown are measured from specially aligned and normalized photographs of the right ear. To normalize and align the images, they are projected onto a standard “Iannarelli Inscribed” enlarging easel which is moved horizontally and vertically until the ear image projects into a prescribed space on the easel. The system requires the exact alignment and normalization of the ear photos as is explained by Iannarelli: Once the ear is focused and the image is contained within the easel boundaries, adjust the easel carefully until the *oblique guide line* is parallel to the outer extreme tip of the tragus flesh line.... The oblique line should now be barely touching the tip of the tragus. Move the easel slightly, keeping the oblique line touching the tip of the tragus, until the upper section of the oblique guide line intersects the point of the ear image where the start of the inner helix rim overlaps the upper concha flesh line area just below the slight depression or hollow called the triangular fosse. When the ear image is accurately aligned using the oblique guide line, the ear image has been properly positioned. The technician must now focus the ear image to its proper size. The short vertical guide line (The right white line in Figure 3.1) on the easel is used to enlarge or reduce the ear image to its proper size for comparison and classification purposes.[21, pp. 83-84]

Since each ear is aligned and scaled during development, the resulting photographs are normalized, enabling the extraction of comparable measurements directly from the photographs. The distance between each of the numbered areas in each ear is measured in units of 3 mm and assigned an integer distance value. These twelve measurements, along with information on sex and race, are then used for identification. The system as stated provides for too small of a

classification space as within each sex and race category a subject is classified into a single point in a 12 dimensional integer space, where each unit on an axis represents a 3 mm measurement difference. Assuming an average standard deviation in the population of four units (i.e., 12 mm), the 12 measurements provide for a space with *less* than 17 million distinct points.Though simple remedies (e.g., the addition of more measurements or using a smaller metric) for increasing the size of the space are obvious, the method is additionally not suited for machine vision because of the difficulty of localizing the anatomical point which serves as the origin of the measurement system. All measurements are relative to this origin which, if not exactly localized, results in all

3.3. DISCRETE WAVELET TRANSFORM

The discrete wavelet transform (DWT) is an implementation of the wavelet transform using a discrete set of the wavelet scales and translations obeying some defined rules. In other words, this transform decomposes the signal into mutually orthogonal set of wavelets, which is the main difference from the continuous wavelet transform (CWT), or its implementation for the discrete time series sometimes called discrete-time continuous wavelet transform (DT-CWT).

The wavelet can be constructed from a scaling function which describes its scaling properties. The restriction that the scaling functions must be orthogonal to its discrete translations implies some mathematical conditions on them which are mentioned everywhere e. g. the dilation equation

$$\phi(x) = \sum_{k=-\infty}^{\infty} a_k \phi(Sx - k). \tag{3.1}$$

where S is a scaling factor (usually chosen as 2). Moreover, the area between the function must be normalized and scaling function must be orthogonal to its integer translates e. g.

$$\int_{-\infty}^{\infty} \phi(x)\phi(x + l)dx = \delta_{0,l} \tag{3.2}$$

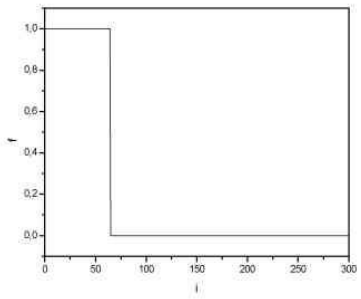
After introducing some more conditions (as the restrictions above does not produce unique solution) we can obtain results of all this equations, e. g. finite set of coefficients a k which define the scaling function and also the wavelet. The wavelet is obtained from the scaling function as

$$\psi(x) = \sum_{k=-\infty}^{\infty} (-1)^k a_{N-1-k} \psi(2x-k) \tag{3.3}$$

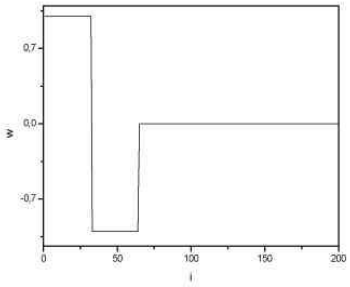
where N is an even integer. The set of wavelets than forms an orthonormal basis which we use to decompose signal. Note that usually only few of the coefficients a_k are nonzero which simplifies the calculations.

EXAMPLES

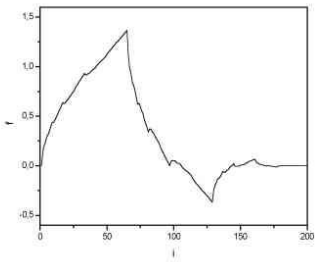
Here, some wavelet scaling functions and wavelets are plotted. The most known family of orthonormal wavelets is a family of Daubechies. Her wavelets are usually denominated by the number of nonzero coefficients a_k, so we usually talk about Daubechies 4, Daubechies 6 etc. wavelets Roughly said, with the increasing number of wavelet coeficients the functions become more smooth. See the comparison of wavelets Daubechies 4 and 20 below. Another mentioned wavelet is the simplest one, the Haar wavelet, which uses a box function as the scaling function.



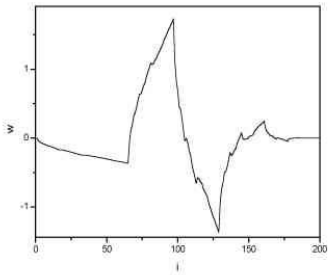
Haar scaling function.



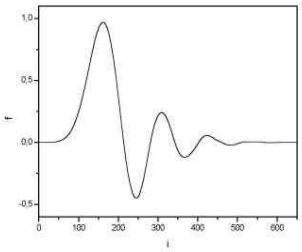
Haar wavelet.



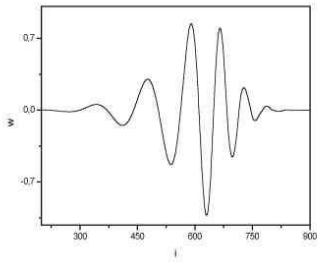
Daubechies 4 scaling function.



Daubechies 4 wavelet.



Daubechies 20 scaling function.



Daubechies 20 wavelet.

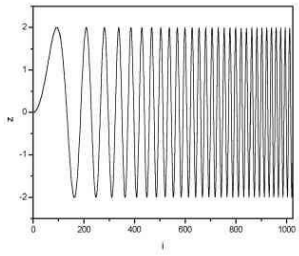
Figure 3.2 Types of Discrete Wavelet Transform

Discrete wavelet transform algorithm:There are several types of implementation of the DWT algorithm. The oldest and most known one is the Malaat (pyramidal) algorithm. In this algorithm two filters - smoothing and non-smoothing one are constructed from the wavelet coefficients and those filters are recurrently used to obtain data for all the scales. If the total number of data D=2^N is used and signal length is L, first D/2 data at scale L/2^(N-1) are computed, than (D/2)/2 data at scale L/2^(N-2), ... etc up to finally obtaining 2 data at scale L/2. The result of this algorithm is an array of the same length as the input one, where the data are usually sorted from the largest scales to the smallest ones.

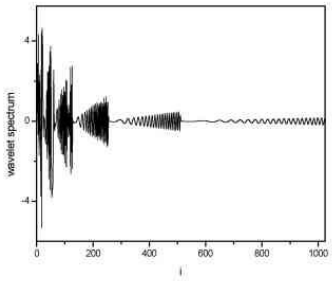
Similarly the inverse DWT can reconstruct the original signal from the wavelet spectrum. Note that the wavelet that is used as a base for decomposition can not be changed if we want to reconstruct the original signal, e. g. by using Haar wavelet we obtain a wavelet spectrum; it can be used for signal reconstruction using the same (Haar) wavelet.

3.3.1 Examples

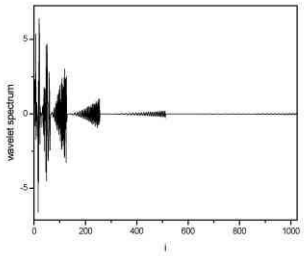
In the next picture a 1024 data long sine signal with linearly increasing frequency. In the next three images there are discrete wavelet spectra obtained using the Haar, Daubechies 4 and Daubechies 20 wavelets as a basis functions.



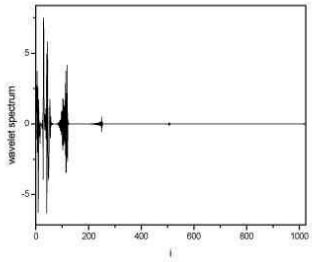
Sine function with increasing frequency.



DWT spectrum using Haar wavelets



DWT spectrum using Daubechies 4 wavelets



DWT spectrum using Daubechies 20 wavelets

3.3 Examples of DWT

From the images above(Figure 3.2) and (Figure 3.3) one can see that the DWT spectrum obtained using Daubechies 20 wavelets has the lowest number of the non-zero terms (or terms significantly above zero). It is a result of the fact that the Daubechies 20 wavelet is the most continuous one of the wavelets used, and, as it is seen from images of the wavelets, it has a form that is most closed to the sine function. Thus, it is logical that the lowest number of such a wavelets is needed to construct the sine signal.

Dyadic grid :We can also plot the data obtained by means of DWT to a 2+1D graph similar to the result of the continuous wavelet transform. As there is not enough of data for doing this in the DWT spectra we have to find out first how to fill the time-frequency plane. This is very simple and it reflects the principal uncertainties of the data obtained in wavelet transform. We simply plot the data into a dyadic grid - a grid that consist of tiles of different width and length depending on actual time and frequency resolution of each partial DWT spectra component. The signal (sine with power of two increasing frequency) DWT spectrum plotted to a time-frequency plane can be seen at the next image (for comparison there is also a result of continuous wavelet transform using a Morlet wavelet which looks more or less similar to the Daubechies 20 wavelet).

3.4 IMAGE HASHING

Image hashing may be defined as the mapping of an image into binary strings. A good hash function generates same hash values for perceptually similar images; images appearing identical to each other should have a high probability of same hash value whereas different images should have different hash values. An image hash function can be used to search and sort an image database, or to select an image from the given database.

We consider the problem of mapping an image to a short binary string, known as image hashing. The image hash function should have the properties that perceptually identical images should have the same hash value with high probability, while perceptually different images should have independent hash values. In addition, the hash function should be secure, so that an attacker cannot predict the hash value of a known image. An image hash function can be used to search and sort an image database, or to select frames in a video sequence for watermark embedding etc.

Here we propose a two stage image hash function. We construct an image hash function by splitting it into two stages. In first step we decompose the input into image into three levels using DWT as given in Section 3.5. Further a hash vector, which should capture the important perceptual aspects of the image, is extracted as given in Section 3.5.3. The hash vectors are

generated for database and query images to perform matching as given in Section 3.5.2. The block diagram for the proposed system is given in 3.5.

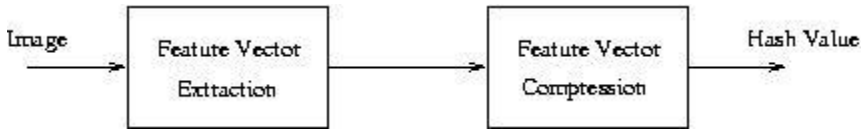
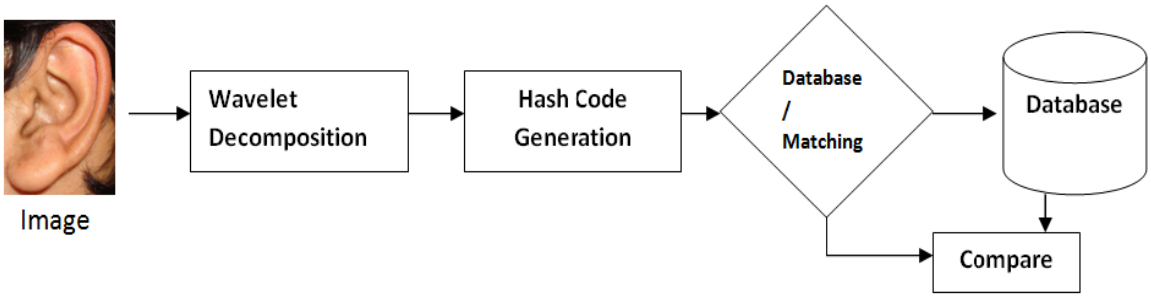


Figure 3.4: Block diagram of image hash function



3.5 Diagrammatic Representation of the Proposed System

3.5 PROPOSED ALGORITHM

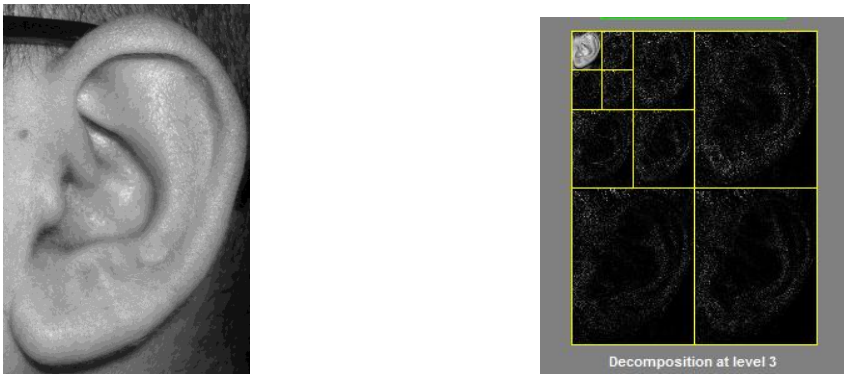
A significant principle behind our design was to allow for the fact that image pixels are strongly correlated and may in fact be modified by an adversary. The detailed description of algorithm is given as follows

3.5.1 Image Decomposition

All wavelet transformations consider a function (taken to be a function of time) in terms of oscillations which are localized in both time and frequency domain. In this experiment discrete wavelet transformation is used as image is represented in the form of discrete matrix. In the

proposed paper Haar Wavelet is used for extracting the features from a polarized iris image. The polarized image of size (80 × 360) pixels is decomposed into five levels using Haar Wavelet transform [21].

The input signal *S* (ear image) is decomposed into approximation, vertical, horizontal and diagonal coefficients using the wavelet transformation and the approximation coefficient (CA_1) is further decomposed into four coefficients. The sequences of steps are repeated to generate a three level wavelet tree. The decomposition of sample ear image is shown in Figure 3.6.



(a) (b)

Figure3.6 Decomposition of (a) Input ear image at (b) three levels

3.5.2 Generation of Hash Code

In this step, image hashing quantization of pseudo random statistics of wavelet coefficients are computed. The image is divided into random rectangles (50 for this system).Inner product of the pseudo random weights generated for the image and the DC sub-band of the wavelet decomposition obtained in the above step of each rectangle generates the hash code.

At first, the image is resized to a square image. The size of the image is reduced by a factor of 8(for level 3 decomposition).The dimensions of the rectangle are obtained randomly. This is necessary to ensure that at each iteration, the sizes of the rectangles are random. Then a linear transform matrix is initialized to zero and uniform weights are assigned to it. The transform matrix is then multiplied by the approximation matrix obtained by the decomposition of the image in the above step. This matrix is quantized to obtain the final hash code.

3.5.3 Matching

The input and query ear images are encoded using the technique given in Section 2.1 and 2.2 respectively. The matching score MS between the two ear images is computed using

$$MS = \left\| \frac{HV_1 - HV_2}{2 * \sqrt{\| HV_1 * HV_2 \|}} \right\| \quad (3.4)$$

where HV_1 is the hash code generated from input image and HV_2 is the hash code generated from query image. ||*|| stands for largest singular value. This matching score is compared against the threshold θ to declare the identity of a person.

3.6 CONCLUSION

Also, we introduce a novel image hashing scheme that is invariant to change in illumination, occlusions and other morphological factors. We use Discrete Wavelet Transform to generate a unique hash code from an image which makes the matching of images with another more robust. There is a scope to further improve upon the generation of robust image hashing techniques.

CHAPTER 4

EXPERIMENTAL EVALUATION

4.1 FEATURE LEVEL CLUSTERING OF LARGE BIOMETRIC DATA

The results are obtained on signature database collected by the authors. The database comprises of signatures from 1000 individuals. Each individual gives nine signatures on a custom defined template. The user is asked to sign within a box. Among the nine signatures available, first six signatures are used for enrollment and last three are used for searching and identification. To measure the performance of the system, bin-miss rate is obtained by varying the number of clusters as shown in Figure 4.1. Bin-miss rate gives the number data that has not fallen into proper cluster. From the graph it is evident that the bin-miss rate increases with increase in the number of clusters (*c*). This implies that by taking two neighboring clusters in case of FCM, poorly whole database is searched for *c* equal to 2. So an optimum value of *c* is required that gives good accuracy with large partitioning of sample space. The comparative study is presented in graph as well as Table 1. From the Table it is evident that when number of clusters is less K-Means performs better as compared to FCM. The reason underlying this is that the hard clustering approaches performs better when database is divided into less number of clusters. However as the number of cluster increases the probability of data lying in a proper cluster becomes very low. Thus use of fuzzy criteria helps in minimizing errors. Here membership grade with pre-computed cluster centers acts as fuzzy criteria.

Table 1 : Bin Miss Rate for different clusters using FCM and K-Means

No of clusters	FCM	K-Means
2	1	0
3	2	0
4	3	1
5	8	8
6	11	12
7	12	18
8	16	21
9	17	25

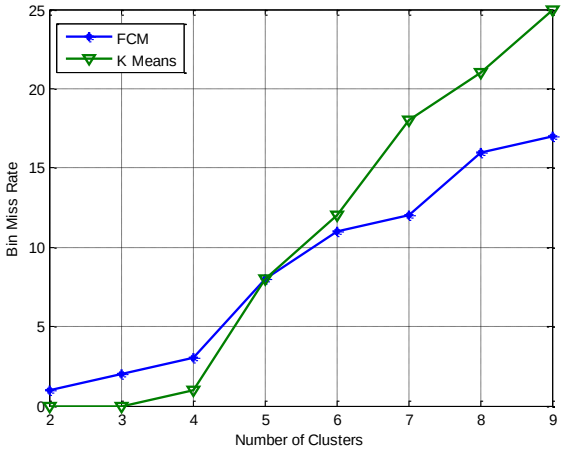


Figure 4.1 Graph showing bin miss rate by varying number of clusters for FCM and K-Means

4.2 DWT BASED HASH CODED BIOMETRIC SYSTEM

Our database has 750 (250×3) ear images of same and different persons. The sample ear database is shown in Figure 4.2. The proposed algorithm tested on our database. The false acceptance rate (FAR) curve and false rejection rate (FRR) curve given here help to choose appropriate threshold. A threshold at 0.05 we are able to minimize FAR which is main concern in ear biometrics. At that threshold accuracy is about 96.37% FAR is 0.17% and FRR is 7.07%.The Receiver Operating characteristic is clearly visible in the ROC curve representation as shown in Figure 4.3. This helps us to understand the consistency of our system. The accuracy versus threshold graph is shown in Figure 4.4.

Figure 4.2 Sample ear database

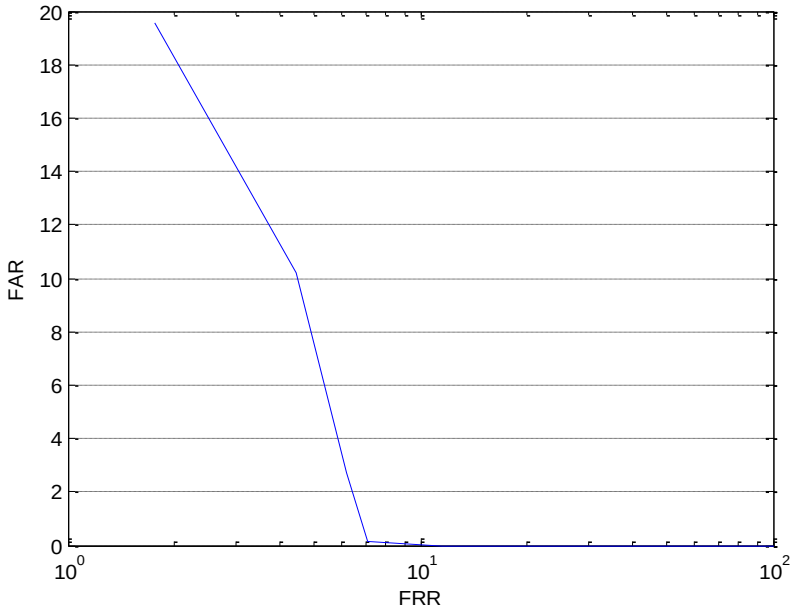


Figure4.3 Receiver Operating Characteristic Curve for the Proposed System

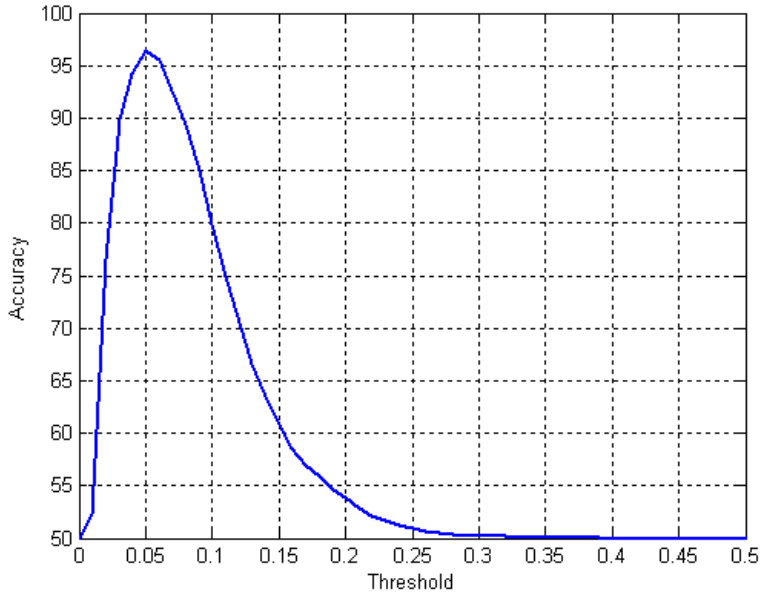


Figure 4.4 Accuracy versus threshold graph of the Proposed System

4.3 CONCLUSION

The proposed identification technique for large databases is an efficient approach to partition the large biometric database, to reduce data retrieval time during identification. The limitations of hard clustering techniques have been removed by introducing the fuzziness criteria. Here fuzziness factor is essential owing to the nature of biometric database. The system is performing comparatively superior as compared to traditional K-Means clustering technique.

The proposed recognition technique based on Discrete Wavelet Transform is an efficient scheme to match images and generate hash codes from images which are robust against compressions and other attacks.

4.4 FUTUTRE WORK

The proposed system can be tested for larger databases and on other biometric traits.
The system may also be tested for scalability issues. To further strengthen the robustness of the system, it may be tested on multiple modalities.

REFERENCES

[1]. Anil Jain,"An Introduction To Biometrics", pp 1-35,2005

[2]. A.Mhatre, S. Chikkerur and V. Govindaraju, "Indexing Biometric Databases Using Pyramid Technique", AVBPA05, pp. 841-849, 2005.

[3]. Y. H. Kwon and N. D. V. Lobo, "Age classification from facial images", Computer Vision and Image Understanding: CVIU, vol. 74(1), pp. 1–21, 1999.

[4]. Z. Sun, G. Bebis, X. Yuan and S. J. Louis, "Genetic feature subset selection for gender classification: A comparison study", Proceedings of the Sixth IEEE Workshop on Applications of Computer Vision, pp. 165–170, 2002.

[5]. B. Moayer and K. S. Fu, "A syntactic approach to fingerprint pattern recognition", Pattern Recognition, vol. 7(1-2), pp. 1-23, 1975.

[6]. L. Yu, K. Q. Wang and D. Zhang, "Coarse iris classification based on box-counting method", In: IEEE International Conference on Image Processing, vol. 3, pp. 301-304, 2005. A. K. Jain, M. N. Murty and P. J. Flynn, "Data Clustering: A Review", ACM Computing Surveys (CSUR), vol. 31(3), pp. 264-323, 1999.

[7]. A.K. Jain and R. C. Dubes, "Algorithms for clustering Data", Prentice Hall, USA, 1988.

[8]. J. C. Bezdek, "Pattern Recognition with Fuzzy Objective Function Algorithms", Kluwer Academic Publishers, Norwell, USA, 1981.

[9]. M. A. Ismail and S. Gad, "Off-line Arabic signature recognition and verification", Pattern Recognition, vol. 33(10), pp. 1727-1740, 2000.

[10]. M. Ammar, Y. Yoshida and T. Fukumura, "A New Effective Approach for Off-Line Verification of Signatures by Using Pressure Features", 8th International Conference on Pattern Recognition (ICPR), pp. 566-569, 1986.

[11]. C.Hui and B.Bhanu, "Human Ear Recognition in 3D", IEEE Trans. Pattern Analysis and Machine Intelligence, 2007, 29(4), pp. 718-737.

[12]. Y.Ping and K.W.Bowyer, "Biometric Recognition Using 3D Ear Shape", IEEE Trans. Pattern Analysis and Machine Intelligence, 2007, 29(8), pp. 1297-1308.

[13]. Y.Li, M.Zhichun, Z.Yu, and L.Ke, "Ear Recognition Using Improved Non-negative Matrix Factorization", Proc. Int'l Conf. Pattern Recognition, China, 2006, 4, pp. 501-504.

[14]. Iannarelli A. Ear Identification. In: Forensic Identification Series. Fremont, USA: Paramount Publishing Company, 1989.

[15]. B.Moreno, Á.Aánchez, and J.Vélez, “Use Outer Ear Images for Personal Identification in Security Applications”, Proc. IEEE 33rd Annual International Carnahan Conference on Security Technology, Spain, 1999, pp. 469-476.

[16]. M.Burge and W.Burge, “Ear Biometrics in Computer Vision”, Proc. Int’l Conf. Pattern Recognition, Spain, 2000, 2, pp. 822-826.

[17]. D.Hurley, M.Nixon, and J.Carter, “Force Field Energy Functionals for Ear Biometrics”, Computer Vision and Image Understanding, 2005, 98, pp. 491-512.

[18]. M.Zhichun, X.Dechun, X.Zhengguang, and Y.Li, “Ear Feature Extraction Combining the Shape Feature of Outer Ear with the Structure Feature of Inner Ear”, Journal of University of Science and Technology Beijing, 2006, 28(5), pp. 497-500.

[19]. A.Iannarelli, *Ear Identification*. Forensic Identification Series. Paramont Publishing Company, Fremont, California, 1989.

[20]. Y.Ping and K.W.Bowyer, “Empirical Evaluation of Advanced Ear Biometrics”, Proc. Empirical Evaluation Methods in Computer Vision, San Diego, 2005, pp. 56-59.

[21]. A.E. Hassanien, J M. Ali: “An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory”. Advanced Modeling and Optimization Journal Vol. 5 (2003) 93-104